REMARKS

The Examiner is thanked for the performance of a thorough search. No claims have been added or canceled. Claims 8-15 have been withdrawn. Claim 20 has been amended to correct an informality. No new matter has been added. Therefore, Claims 1-7 and 16-13 are pending in the application.

Each issued raised in the Office Action is addressed hereinafter.

I. ISSUES NOT RELATED TO THE PRIOR ART

A. CLAIMS 25-31 – OBJECTION TO INFORMALITY

Claims 25-31 are objected to because of alleged informalities. The Office Action alleges at page 2 that the term "computer-readable storage medium" recited in Claims 25-31 is not defined in the specification. The objection is respectfully traversed.

An artisan of ordinary skill would understand in light of general knowledge in art at the time the invention was made that the term "computer-readable medium" refers to any medium that participates in providing data that causes a computer to operate in a specific fashion. The artisan would further recognize that such medium can take many forms, including storage media and that storage media includes both volatile and non-volatile media. Non-volatile media includes, for example, optical or magnetic disks. Volatile media includes dynamic memory, such as the main memory of a computer. For example, Figure 2 of the present application shows a computer-readable storage medium Memory 214 which includes "high-speed random access memory and may also include non-volatile memory, such as one or more magnetic disk storage devices." quoting Specification, paragraph 32. Therefore, the specification discloses computer-readable storage medium. Applicant respectfully requests removal of the objection.

II. ISSUES RELATED TO THE PRIOR ART

A. CLAIM 1 – 35 U.S.C. § 102(e) – PTACEK

Claim 1 stands rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Ptacek, et al. (U.S. Pub# 2005/0005017) (hereinafter "Ptacek"). The rejection is respectfully traversed.

To anticipate a claim, the cited reference must teach each and every element of the claim. MPEP § 2131. As explained hereinafter, Claim 1 recites at least one feature that is not disclosed, taught, or suggested by *Ptacek*.

Claim 1 features:

> "A method of analyzing security events, comprising:
> receiving and processing security events, including grouping the security events into network sessions, each session having an identified source and destination;
> **displaying** a graph representing devices in a network, the devices including security devices and non-security devices, the displayed graph including a plurality of individual device symbols and **a plurality of group device symbols**, each individual device symbol representing a security device of the network and **each group device symbol representing a group of non-security devices of the network**; and
> **displaying** in conjunction with the graph **security incident information**, including with respect to a group device symbol an **incident volume indicator** that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol." (Emphasis added.)

Thus, Claim 1 features displaying a graph representing security and non-security devices in a network and displaying in conjunction with the graph security incident information and incident volume information. In the displayed graph, a plurality of group device symbols is displayed wherein each group device symbol represents a group of non-security devices in the

network. None of the art of record discloses or in any way renders obvious these features of Claim 1.

In contrast, *Ptacek* discloses a technique for protecting a communications network from a network attack, such as from a "worm", without jeopardizing legitimate network services. Figure 1 of *Ptacek* shows a static communications network configuration typical of a large enterprise in which the invention disclosed in *Ptacek* may be implemented. *Ptacek* does not disclose displaying the network configuration. Figure 1 is merely a patent application block diagram that illustrates an exemplary computer network and is not displayed as a result of process or method steps. Thus, reproducing a patent drawing in a patent or patent application is not a 'displaying' step within a process, as claimed.

Assuming, for the sake of argument only and not in any way as an admission as to the disclosure of *Ptacek*, that Figure 1 of *Ptacek* is displayed as a result of process steps, *Ptacek* does not disclose, teach, or suggest displaying a plurality of group device symbols where each group device symbol represents a group of non-security devices of a network. The Office Action alleges that the displaying a plurality of group device symbols feature of Claim 1 is disclosed by Figure 1 of *Ptacek*. Office Action, page 3. This is incorrect. Figure 1 of *Ptacek* shows a plurality of security and non-security devices in a network where each device is singularly represented by a device symbol. For example, the symbol associated with Disk Array 14 of Figure 1 of *Ptacek* represents a single disk array device and each of the symbols associated with Client 10 in Figure 1 each represent a single client device. Figure 1 does not show a symbol that represents more than one device. Therefore, *Ptacek* does not disclose, teach, or suggest displaying a plurality of group device symbols, each group device symbol representing a group of non-security devices of a network.

Further, *Ptacek* does not disclose, teach, or suggest displaying security incident information in conjunction with displaying a graph representing devices in network as featured in Claim 1. The Office Action alleges that figure 1 of *Ptacek* discloses this displaying feature of Claim 1. Office Action, page 3. This is incorrect. Figure 1 of *Ptacek* is a static network diagram that shows how devices in the network are logically configured. For example, Figure 1 of *Ptacek* shows subnet 1 which includes SQL Server 12-2 and SQL Server 12-1 connected to switch 20-1. Figure 1 of *Ptacek* does not show any concerted network activity between two or more devices. It merely shows how the devices are logically related to each within the network. Therefore, Figure 1 of *Ptacek* does not disclose, teach, or suggest displaying security incident information in conjunction with displaying a graph of representing devices in network as featured in Claim 1.

Further, *Ptacek* does not disclose, teach, or suggest displaying incident volume information in conjunction with displaying a graph representing devices in network as featured in Claim 1. Notwithstanding that Figure 1 of *Ptacek* does not show a group device symbol that represents a group of non-security devices, Figure 1 does not show incident volume information that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices. The Office Action alleges that the display of incident volume information feature of Claim 1 is disclosed in Figure 1 of *Ptacek* and at page 3, paragraphs 32-38 of *Ptacek*. However, nowhere in these portions of *Ptacek* or elsewhere is it disclosed displaying incident volume information that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices. A network session as disclosed in the present application is a group of security events sharing a same set of session qualifiers including, but not limited to, source address, destination address, and network protocol. At best, the signatures taught by *Ptacek* in paragraph 65 can be said to correspond to the network sessions

of claim 1. However, the signatures disclosed in *Ptacek* do not group security events in the network nor is there an indication of the number of signatures whose source or destination is at any member of a group of non-security devices displayed on a graphical user interface. Therefore, *Ptacek* does not disclose, teach, or suggest the displaying incident volume information feature of Claim 1.

Finally, *Ptacek* does not render Claim 1 obvious because there is no teaching or suggestion in *Ptacek* that would have motivated one skilled in the art to modify *Ptacek* so as to realize the features of Claim 1. For one, *Ptacek* is directed to techniques for protecting a network from network attacks and not to efficient display of network security incidents in a graphical user interface. Indeed, there is no mention of a display at all in *Ptacek*. Further, grouping non-security devices would change the principle of operation of *Ptacek* which is directed to protecting individual devices in a network from an attack. To that end, the invention in *Ptacek* creates a "usage model" of the normal operation of the network by capturing individual packets sent between non-security devices in the network. See Ptacek, Figure 1, element 115 and accompanying discussion in the specification. Each packet is recorded in a signature database identified by a timestamp and the address of the sending non-security device and the address of the receiving non-security device. Ptacek, paragraphs 53-70. During a network attack, the invention disclosed in *Ptacek* can detect whether a network flow between two non-security devices is abnormal by comparing it to the signatures captured in the usage model. Grouping non-security devices as disclosed in Claim 1 would require a substantial reconstruction and redesign of the usage model disclosed in *Ptacek* as well as a change in the basic principle under which the invention in Ptacek was designed to operate. Therefore, Claim 1 is not obvious in view of *Ptacek*.

Because *Ptacek* fails to disclose, teach, suggest, or in any way render obvious the features of Claim 1, the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 16, 17, 18, 25 – 35 U.S.C. § 102(e) – PTACEK

Claims 16, 17, 18, and 25 contain features that are similar to those described above with respect to Claim 1, and in particular all feature the "displaying" features of Claim 1. Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 16, 17, 18, and 25 are allowable over the art of record and are in condition for allowance.

C. REMAINING CLAIMS – 35 U.S.C. § 102(e) – PTACEK

The pending claims not discussed so far are dependant claims that depend on an independent claim that is discussed above. Because each dependant claim includes the features of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable. Removal of the rejections with respect to the dependant claims and allowance of the dependant claims is respectfully requested. In addition, the dependent claims introduce additional features that independently render them patentable. Due to the fundamental differences already identified, a separate discussion of those features is not included at this time.

III. CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Please charge any shortages or credit any overages to Deposit Account No. 50-1302.

Respectfully submitted,

Hickman Palermo Truong & Becker LLP

Date: November 9, 2007

/AdamCStone#60531/

Adam Christopher Stone
Reg. No. 60,531

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 231
Facsimile No.: (408) 414-1076